BBT
BEYOND
BROADBAND
TECHNOLOGY

April 1, 2011

Julius Genachowski
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20054

Re: ***Video Device Competition*, MB Docket No. 10-91; *Commercial Availability of Navigation Devices*, CS Docket No. 97-80; *Compatibility Between Cable Systems and Consumer Electronics Equipment*, PP Docket No. 00-67**

Dear Chairman Genachowski and Commissioners Copps, McDowell, Baker, and Clyburn:

Over the past several years, Beyond Broadband Technology (BBT) has actively participated in various Commission proceedings relating to the implementation of Section 629 of the Communications Act, including Docket 97-80 (the "CableCARD" proceeding) and Docket 10-91 (the "AllVid" proceeding). The focus of our participation in these proceedings has been on the necessity for, and challenges presented by, the development of a uniform, open, downloadable security solution for both video and data transmitted over cable broadband systems. As we have reported in previous filings and meetings with the Commission, *BBTSolution*® cable set-top boxes that offer a workable downloadable security solution are now being deployed. However, as recent events have demonstrated, it is essential that the Commission understand the complexity of the security issue and of the need for a carefully delineated approach to that issue in any new actions that the Commission proposes or takes in this arena.

Specifically, it has recently been reported that two widely used methods for securing video and data have been compromised. Intel, developer of the HDCP (High Definition Content Protection) protocol, which is an integral part of DLNA (Digital Living Network Alliance), has confirmed that it suffered a major security breach when its "root key" for security was published on the Internet. And just last week, RSA Security announced that it, too, had experienced a significant security threat to its broadly used SecureID system. The vice president for information security and cryptography at the Internet Corporation for Assigned Names and Numbers (ICANN), Whitfield Diffie (described in a New York Times article on the breach as "a computer security specialist who was an inventor of cryptographic systems now widely used in electronic commerce"), was quoted as saying it was possible "a 'master key' — a large secret number used as part of the encryption algorithm — might have been stolen."

These recent events illustrate a point that BBT has previously sought to make in a "White Paper" submitted to the Commission in both Docket 97-80 and Docket 10-91 (and attached here for the Commission's convenience). As explained therein, it is critical that the Commission exercise great care in the language it uses to describe what, exactly, it is seeking in order to meet the requirement for "separable security." In particular, the Commission must, as it considers whether and how to proceed in implementing the "AllVid" proposal, make clear that it understands the distinction between the concepts of "separable security" and "secure communications paths" on the one hand and "conditional access" and "DRM" (digital rights management) on the other. The latter two terms refer to methods of placing restrictions on who can access given data (including, of course, video) and placing conditions on the method and use of that data. In contrast, a secure communications path is a means of assuring that whatever data is being transmitted goes only to the party it is intended to reach, regardless of the additional conditional access, encryption, or rights management appended to it.

In the past, the Commission unfortunately has blurred the distinction between these concepts by, for instance, citing DCAS (downloadable conditional access system) as an example of "downloadable security." Downloadable conditional access itself does not assure the more fundamental requirement of a secure communications path (usually referred to as a "secure authenticated channel" or "SAC"). As the White Paper explains, these two distinct elements of a workable security solution are accomplished by different means. For example, in the case of the *BBTSolution*®, these two elements are separated: a very sophisticated, versatile and inexpensive secure microchip is used to create a secure communications path while a non-proprietary mechanism allows multiple conditional access or DRM protocols to be downloaded and employed (downloadable security).

By separating the secure communications function from the conditional access function, BBT has succeeded not only in designing a new method of creating a secure authenticated channel, but also has avoided what appears to be the major weakness that has been targeted in current security systems: the reliance on a "root key" that must be utilized through a "trusted authority" to create the SAC. The BBT approach does not require a centralized "trusted authority" and thus there is no risk of a centralized data breach, as Mr. Diffie apparently fears happened in the RSA situation. There is also no static "private key" that must be used to create the secure communications path, as is the case with HDCP. Discovery and publication of that private key has now potentially opened the door to video data breaches on millions of HDMI-enabled devices which rely solely on HDCP for security. Although the Commission previously has suggested that the DLNA/HDCP/HDMI model might be the appropriate one for a mandated "AllVid" device, such a choice obviously would now be problematic.

We are again raising these issues in the hope that the Commission will more carefully distinguish among the base-line security issues that it needs to address in any further proceedings it may undertake relating to the AllVid proposal. BBT has made clear in prior filings that we do not think it wise for the Commission to adopt technology mandates for MVPD set top boxes or "gateways" or for the security elements that are inherently a part of such an exercise. In an area of technology as volatile and rapidly evolving as this one, any effort at "standardizing" not only will stifle innovation, but also will create a larger threat target (potentially consisting of all of the new standardized devices) that will prove irresistible to hackers and others that seek to breach the security of cable broadband networks.

The issues that we raise here and in the White Paper with respect to the need to distinguish between a secure communications path and downloadable conditional access are part of a rapidly evolving and complicated field. For example, Cablevision Systems Corporation has announced its intent to deploy a "downloadable" security system (referred to variously as "OMS" (Open Media Security), "K-Lad" (KeyLadder), or "JCAS" (Java Conditional Access System)). This approach requires large reserves of bandwidth and headend processing capacity. Further, it still relies on a "trusted authority" and on embedded, static keys, both of which can lead to the type of headlines we referred to above.

This is not to say, however, that the "OMS" approach is bad, or that it is wrong for Cablevision, whose systems have the required bandwidth reserves and headend processing capacity, to pursue this solution. But it could not likely be employed in most other systems that lack those luxuries. Moreover, such a proprietary design accomplishes a different task, and thus should not be conflated with the BBT design of a secure authenticated channel that is autonomous and separable from additional capability to download alternative conditional access and/or DRM protocols.

The *BBTSolution*® (which is platform agnostic and can work on both QAM and Internet Protocol systems) and "OMS" represent two new, but totally different approaches to the challenge of securing data and both have their place. As suggested above, regardless of one's view of the wisdom of a government effort to standardize or require a given technical methodology for the uniform delivery of video by all MVPDs, there can be no argument that whatever the method, security is critical to it. The issues relating to securing data all the way to the consumer's television screen or other device are separable, controversial and complicated. Without that security no standard will succeed. These issues have to be addressed very carefully if the Commission intends to get useful input.

We look forward to having the opportunity to discuss this matter with the Commission in advance of any decision on the direction of the AllVid proceeding.

Sincerely,

Bill Bauer

cc: Commissioner Copps
Commissioner McDowell
Commissioner Baker
Commissioner Clyburn
William Lake
Steven Broeckaert
Michelle Carey
Lyle Elder
Mary Beth Murphy
Nancy Murphy
Brendan Murray
Alison Neplokh
Doug Sicker
Marlene H. Dortch

Beyond Broadband Technology / The BBT*Solution*™

A "WHITE PAPER" ON A NEW CONCEPT FOR SECURING THE TRANSMISSION OF ELECTRONIC INFORMATION

Beyond Broadband Technology, LLC, (BBT™) has developed The BBTSolution, an open standard downloadable security system which does not require the use of a "trusted authority." The BBTSolution constitutes a unique method of establishing a secure communications path with either one-way or two-way devices as well as mechanisms for establishing authentication, authorization and reception of encrypted transmissions of voice, video or other data.

Explaining a new concept in the field of information security is never easy. That's particularly the case since various users, purveyors, government regulators and even standards-setting bodies use either very similar or very conflicting definitions for similar terms. This "White Paper" is meant to make clear what we are referring to with the terms being used to explain the BBTSolution, and thereby help to underscore the unique flexibility it can bring to multiple forms of information security.

INFORMATION SECURITY

This is a very broad term, and in the context of the BBTSolution, it is meant that way. The BBTSolution establishes a highly secure communications path between a transmitting device and a receiving device. The transmission medium is not restricted. As is explained below, the BBTSolution was first designed for use with cable television broadband systems. However, this OSDS (open standard downloadable security system) is not restricted to any particular communications path, and will also work on IP (Internet Protocol) systems or over-the-air, satellite or other transmission paths just as well. Once a secure, authorized and authenticated communications path is established, the system is totally agnostic to the type of data, or information, transmitted over that path. Thus when we talk about "information security," it could be anything from a television program or channel, or first-run movie to health care or banking information, automated data for controlling the power grid, or any other type of information.

Once the secure communications path is established, the level of security, including authentication, usage restrictions, or any other type of security is user-definable. What makes this approach unique is that because it is "downloadable," security conditions can be changed repeatedly, depending on the use. In other words, it can be employed by multiple transmitters of information, each utilizing different types and levels of security. A consumer with a BBTSolution enabled computer (either built-in or in a portable USB "dongle") for instance, could securely access multiple video programmers via the Internet, each with its own encryption and conditional access protocols. A Veteran could have similar access to all his or her medical records at multiple locations with total security provided by a BBTSolution chip in a USB thumb-drive type device, or embedded in medical facility computers.

THE BASICS

The BBTSolution has two parts: a secure microchip in the receiving device, and an "HSM" (Hardware Security Module) at the transmitting site. The HSM can be integrated into the transmitting location of a cable broadband, satellite, broadcast or telephone system, or it could be a part of any computer server used by a provider of information on the Internet, for instance. HSMs could also be integrated into devices (such as a host computer) used by doctors or hospitals to transmit patient data or any other data transmission application. The cost of the HSM enabled equipment will vary depending on the use. The current design for cable television systems, including the computer, costs less than $10,000, approximately one-tenth the price of the conditional access headend controllers commonly used in that market today. We anticipate that the basic Hardware Security Module enabled for use on computer servers can cost half that, or even less.

The secure microchip can be incorporated into, as examples, a cable television set-top box, a television set, a digital video recorder, a home, office or laptop computer, or even in a portable USB device (much like a "thumb drive" or "dongle") that could be inserted in any current computer USB port. The chips, which are already being manufactured by one of the best-known secure microprocessor manufacturers in the world, ST-Microelectronics, are inexpensive (they are currently priced at $5.00 including the BBT license fee) and are designed to be integrated into multiple consumer devices, much like the well-known "Dolby™" system is included in most consumer audio devices today.

BOTH TWO-WAY AND ONE-WAY DEVICES

One of the many unique aspects of the BBTSolution is that the receiving device, such as a television set, need not be a "two-way" device. The secure communications path, once established, is totally managed by the transmitting and receiving devices themselves, and the receiving device does not have to be in constant return-path communication with the transmitting HSM enabled equipment. Thus, for instance, with one telephone call a cable television consumer could read a series of numbers that appeared on their television screen to the headend and from that point on the cable HSM enabled headend controller and the consumer's BBTSolution device can establish and maintain a secure authenticated channel (SAC) without the need for two-way communication or bandwidth use. Of course the system will also work, automatically, with two-way communications, such as with IP computer communications on the Internet or in two-way broadband cable systems.

THE ORIGINAL CHALLENGE

The BBT*Solution* was originally designed to respond to a need for a new, low-cost cable television set-top box that could meet government mandates for "separable security" for such devices. Until June of 2007, cable television systems traditionally used a set-top box (a tuner and descrambler) that had "integrated security." That is, the entire process of assuring that the box belonged to the right customer, was in the right location, and had the proper codes to decrypt only that programming meant for that customer was all integrated into the set-top box. Legislation intended to foster a consumer market for set-top boxes resulted in the FCC establishing rules requiring that the security function be separated from the rest of the functions of the set-top box. This, theoretically, would allow anyone to design new and competitive set-top boxes that could be used in any cable system since the security function was not integrated into the box and could be enabled in each location (which had different security, or "conditional access" systems) another way.

The method originally chosen for this separated function was the CableCARD, a modified version of the PCMCIA (Personal Computer Memory Card International Association) card then in use in personal computers. The idea was that any set-top box could be built with a capability to accept the CableCARD, and that cable systems could supply the appropriate card, which controlled the security, or what has generally been called the "conditional access" components of the system. Unfortunately, CableCARDs are both expensive (both the card and the docking device) and no longer constitute an advanced technology. The PCMCIA design is generally now considered obsolete, and most computers today no longer incorporate PCMCIA slots, having progressed to new designs such as USB (Universal Serial Bus). The BBTSolution is, however, "backward compatible" with CableCARDs.

One of the original objectives of BBT was to design a new "separable security" system. Several efforts to design such a new system were launched by various companies. Unfortunately, the layman's language used to describe these systems, which was subsequently adopted by the FCC, was "downloadable conditional access systems" or DCAS. We say unfortunate, because this language necessarily confuses the various functions being described, and implies that they are all part of a single, integrated process. While that is a traditional approach to security and conditional access, it is not the only way it can be accomplished. Another of the unique attributes of the BBTSolution is that it separates the establishment of a secure communications path from the other functions of authorization, authentication and encryption/decryption of the data. This allows, as is explained below, almost unlimited flexibility in the use of the system.

A SECURE COMMUNICATIONS PATH -- WITHOUT THE NEED FOR A "TRUSTED AUTHORITY"

The traditional approach to establishing a secure communications path is to use a "public/private encryption key" dialog between devices. However this standard approach also requires that the "private key" be in some way secured and archived for referral and use to authorize the communication. Thus, there must be a "trusted authority" holding and controlling all of the private keys. If those keys are somehow discovered, the entire security system, including all the devices with hardware linked to those keys, if any, are compromised. The BBTSolution does not employ public/private keys or require a "trusted authority," thus eliminating the two most significant vulnerabilities of the traditional approach.

With the BBTSolution, the "public/private" keys that enable devices to securely communicate are replaced by a "symmetrical key" approach. Keys are determined internally by the HSM and the secure micro embedded in the receiving device. Each time the HSM and a receiving device establish a secure communications link new random keys are used, thus there is no need for a "trusted authority" and the risk factor of "hacked" or stolen keys is eliminated. No user needs to rely on any other entity for the maintenance of security of the devices used in its communications. This, in turn, significantly reduces the "threat target" for secure communications. Since each user of the BBTSolution establishes their own conditions for authentication and use, what we term "conditional access," the two parts of the security protocol; establishing the secure communications path and then establishing the authentication, access and use conditions, become additive in their security effect, particularly since they are not static.

DOWNLOADABLE CONDITIONAL ACCESS

The basic BBTSolution does not include "conditional access" protocols. The entire idea behind the early development of this approach, as noted above, was to separate the establishment of the secure communications path from the conditions imposed on the use of data after that communications path was created. Thus, the BBTSolution has been designed in an "open" format where specifications will be made available so that anyone can design "conditional access" software that can be downloaded to the receiving BBTSolution-enabled device. This conditional access software can be as simple or as robust as the user chooses. For instance, in the case of a cable television system operator, the conditional access system might be automatically triggered by a known subscriber code number, pin number, or location address. In the case of a portable USB "stick", which could be inserted in any modern computer at any location, a program supplier (ESPN or a movie supplier, as examples) could, once the secure communications path is established, download a customized "conditional access" protocol that required a password, a credit card verification, or some other method of authentication. The relationship between the information provider and the customer over the Internet would be direct, and totally controlled by the conditions imposed by the intellectual property owner. In the case of medical records, it has already been suggested that the USB key or an embedded secure micro at the medical facility could be conditioned to be authorized only with thumb print verification, as well as a password to assure security and privacy of personal data.

Once the BBTSolution secure communications path is established, the conditional access protocol of the given information provider is downloaded, and authentication has taken place, then the information distributor can additionally impose any other conditions for the access of the material being sent. Of course at minimum, that information is encrypted. The BBTSolution secure micro includes a "virtual machine" or "tool box" that contains over a dozen of the most commonly used encryption algorithms. These algorithms have all withstood the test of time and have proved to be highly secure. But in the BBTSolution approach they are even more so, because they can be used in any order and any combination, again at the discretion of the information provider. Thus, a conditional access protocol could be downloaded instructing the BBTSolution secure micro to use, assuming, for instance, if there were 12 algorithms available, any combination of 12 to the 12th power combination of encryption/decryption processes. However one can never assume that something simply can never be "broken," so the system is designed so that the protocol can be changed at will by the provider, as many times as they wish, and as often as they choose. It is generally acknowledged that a "software-only (DRM--"digital rights management") approach to encryption or conditional access is subject to constant challenge. As the saying goes, "...there's a new crop of 18-year-old hackers every year!" The BBTSolution HSM and microchip, along with a downloadable conditional access component, does not suffer from that same risk. It is a highly adaptable, nimble and very flexible approach to secure communications.

Along with establishing security and conditional access, including any form of additional "DRM" chosen by the information provider, the ability to "download" protocols allows for other flexibility as well. For instance, information stored in different formats may require that a "reader" be associated with the information being transmitted. This is particularly true in a field such as health care. Reader programs, with limitations on use, both in terms of time and content, could be downloaded and deleted with each session establishing a secure communications path. Data downloaded to a computer hard drive could be stored only in encrypted form, thus totally protected unless a secure communications path was established to authorize decryption.

CONCLUSION

The BBTSolution is unique. It allows for absolutely secure communication and control of intellectual property and privacy of data transmissions on multiple broadband and narrowband formats. It can enable such communication to devices that are either one-way or two-way capable. It does not require a "trusted authority" and allows for maximum flexibility for individualized conditional access and use. It's potential uses for broadband and the Internet, in particular, can fundamentally change the way those platforms are used today.

ADDENDUM ATTACHED

ADDENDUM – I

Recent events have highlighted the validity of the reasoning behind the BBTSolution™ approach to electronic information and communications security. The experimental "hacking" of the latest proposed algorithm for use in 3G cellular telephony and the increased focus on illegal international efforts to access proprietary data from various secure repositories of corporate information has once again demonstrated the weakness in current security thinking. The vulnerability recently reported regarding RSA's "SecurID," and the publication of the root key for HDCP (High Definition Content Protection) reinforces this point. Software solutions and "secure repositories" or "trusted authorities" are being challenged regularly and there is no indication that this activity will stop. A recent article in the New York Times, "Experts Warn of a Weak Link in the Security of Web Sites" (8/13/10), focuses specifically on the issue of "trusted authorities" that the BBTSolution seeks to address.

The BBTSolution™ answer to that challenge is a design where any attack on the system is anticipated, repairable, and totally limited. There is no "trusted authority." The "threat target" in the BBT approach can be reduced, literally, to single communications events. Each initiation of the BBTSolution™ secure communications path utilizes a totally unique and individualized creation of ephemeral keys. Those keys would have to be broken during the immediate initiation of the communications session, since once the individual session is over those keys are no longer of any relevance. Further, since each session and associated conditional access protocol is totally controlled (as to timing, duration, content, encryption, etc.) by the communicating parties, they can change any or all parameters at will. A "hacker" would have to, while the communications session was in progress, ascertain all of those variables, including the methodology and algorithm used for deriving the unique session keys. Portions of that methodology and the algorithms used are variable as well, making any single session "hack" of very limited value.

Rather than try to create a "Fort Knox" that "can't be broken into," BBT has taken a totally different approach, creating a security design that is so nimble and flexible that the extreme effort it would take to compromise the secure communications path could only yield a result, if successful at all, for that single, unique communication. In addition, all system administrators create their own set of variables, encryption and additional conditional access protocols, adding to the overall security for the vast majority of uses.

A REPRESENTATIVE EXAMPLE: ELECTRONIC MEDICAL RECORDS

There are several interrelated issues in the effort to shift to electronic medical records. Not only is individual security and privacy required, but the records themselves, as in the case with the Veterans Administration, for example, may be in different locations and they may not all be uniform. The use of the BBTSolution™ downloadable security design can address all of those challenges.

In order to assure privacy and authentication, a BBTSolution™ secure microchip can be embedded in a personal "USB Dongle" (a form-factor like a "thumb drive") which also incorporates a biometric (thumb print) reader. The veteran could then visit any facility with computers having USB inputs and authenticate his or her right to access the particular medical records by establishing a secure communications path with any repository medical computer having the requisite HSM (Hardware Security Module). The encrypted thumb print data is stored directly on the resident secure microchip. The USB device will not establish any secure communication without that initial authentication. Any additional authentication required, such as a password, an account number or whatever the institution requires with its own pre-established set of conditional access rules, which would be downloaded to the receiving computer upon initiation of the secure communications path, would assure that the encrypted records were only being transmitted to the appropriate location and that only that location had the requisite information to decrypt the files. That decryption capability would, in this example, only last as long as the secure communications path was in place.

The process also anticipates the interim "downloading" of specialized software should the sending and receiving medical facility not have the same capabilities for reading or reviewing the records. It, too, would only be useable so long as the secure communication path was intact, or limited in any other way decided upon.

Of course, any other set of variables could be applied to the medical data thus downloaded. It could be time limited and then automatically discarded, it could be decrypted or left entirely encrypted and only accessible during secure communications path sessions with the personalized USB key, or it could be authorized for use by the new medical facility as a repository for the data. All of these options and many more can be made available through the use of easily developed and downloaded computer code. The key to the secure communication of the data is the initialization of the secure communications path, and the multiple options afforded the user through downloadable capability once that path is established.

While we have cited a USB thumb-drive type form factor (currently tested and ready for mass production) in this quick exploration of how the BBTSolution™ can be used to address many of the challenges of electronic health care records security and distribution, there are other form factors that could also be employed, such as a "smart card," or the BBT secure microchip being directly incorporated into a computer laptop. In addition, it should be noted, again, that because of the flexibility inherent in the downloadable design, the same chip (in whatever form factor) used for securing electronic medical records, for instance, could also be used to view a movie, download a book, or do anything else requiring an authenticated secure communications path to multiple devices such as computers, laptops, television sets, game consoles, etc.

The whole point behind this (patent pending) approach to broadband IP security is that it can be used for multiple purposes and each one can be secured in a different way with as much or as little additional conditional access as is deemed necessary by the parties establishing the communications path. Each communications session is unique as to use, content, authentication and any other conditions chosen based on the nature and need of the communicating parties. Because of that flexibility and versatility, the BBTSolution™ security protocol enables far more uses in a more secure manner than current designs.

03 25 11
Contact: Steve Effros
steve@effros.com
703-631-2099